Lab 1. CyberCIEGE Macro Viruses

CyberCIEGE is an information assurance (IA) training tool that illustrates computer and network security principles through simulation and resource management trade-offs. CyberCIEGE players construct computer networks and make choices affecting the ability of these networks and the virtual users to protect valuable assets from attack by both vandals and well-motivated professionals.

It is anticipated that the student has first played the “Stop Worms” scenario.

This “Life with Macros” scenario explores the following concepts:

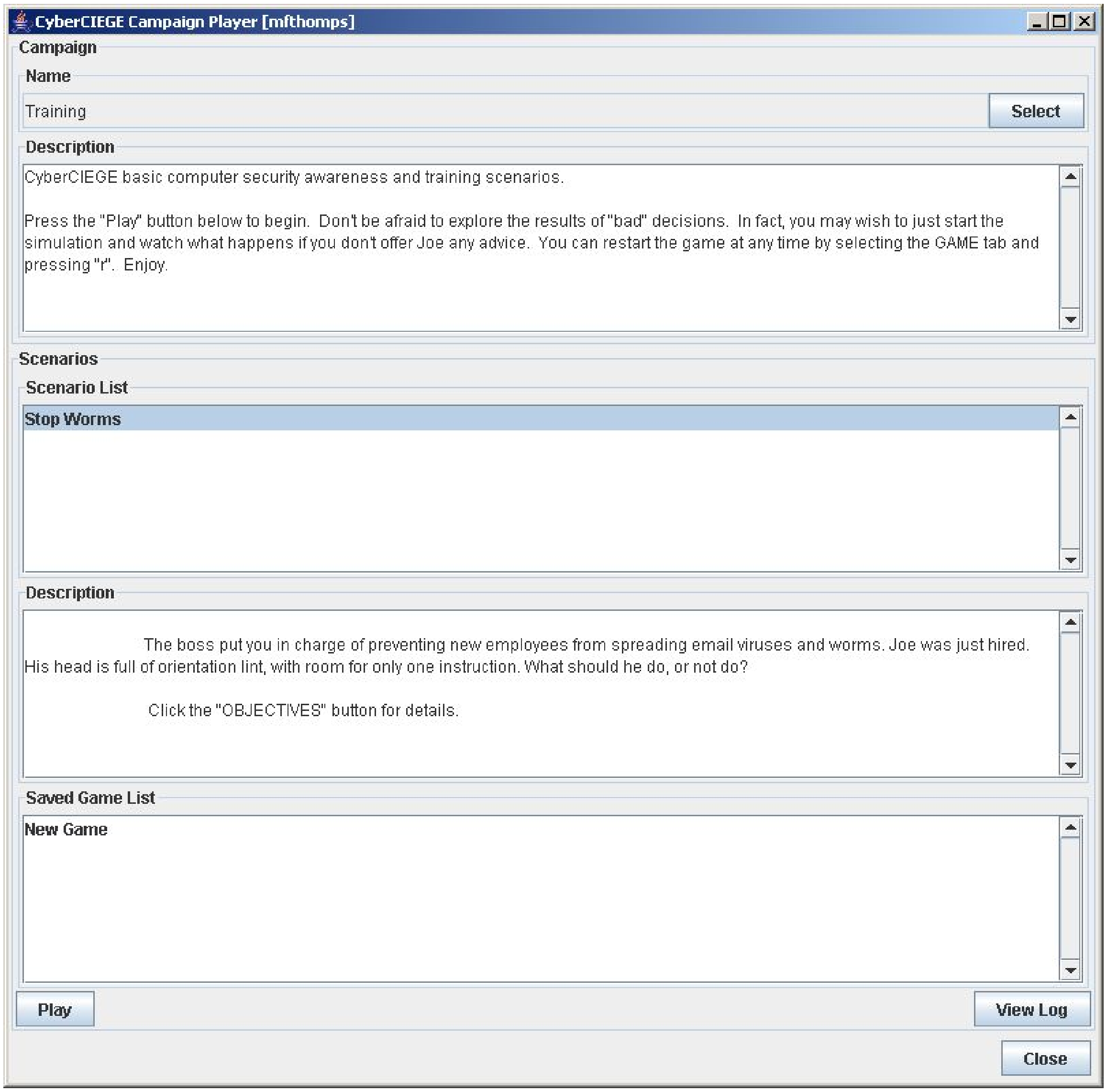
- Some document formats, e.g., word processing and spreadsheets include a feature called “macros” that extend the functions of the applications and automate tasks.
- Macros can be malicious in nature and can propagate to other documents.
- Some organizations must handle documents that may contain macros, and the source of these documents cannot necessarily be trusted to not distribute macro viruses.
- Use of up-to-date antivirus tools can reduce the risks of macro viruses.

In this scenario you can largely ignore Zones and physical security issues. The scenario requires that you modify only one procedural setting on one computer. Also, don’t worry about hiring or firing support staff or the trustworthiness of your virtual users.

1.1 Preparation

The game is installed in the 3600 lab and is available from the workstations.

> From the CyberCEIGE folder on the desktop, open the “Training” icon.   This will start the “Campaign Player” seen in figure 1.



Campaign

Name: Training

Description:

CyberCIEGE basic computer security awareness and training scenarios.

Press the "Play" button below to begin. Don't be afraid to explore the results of "bad" decisions. In fact, you may wish to just start the simulation and watch what happens if you don't offer Joe any advice. You can restart the game at any time by selecting the GAME tab and pressing "r". Enjoy.

Scenarios

Scenario List: Stop Worms

Description:

The boss put you in charge of preventing new employees from spreading email viruses and worms. Joe was just hired. His head is full of orientation lint, with room for only one instruction. What should he do, or not do?

Click the "OBJECTIVES" button for details.

Saved Game List: New Game

Figure 1: Read the Campaign Description and Click Play

Read the campaign description. Then click the “Play” button.

1.2 Play

1.2.1 Watch Bad Things Happen

Click the OK button in the initial briefing.
Click the play button to begin the scenario (a help balloon text will appear to show you the play button.)

In your first time through, don't make any configuration changes. Just press the "esc" key to move past each balloon text. Don't even bother to click the "Objectives" button. See what happens if you just let the scenario progress.

After the pop-up dialog explains what has happened, simply restart the game by selecting the GAME tab and pressing the "r" key.

1.2.2 Play the Scenario to Succeed

Now play the game again. This time, after pressing the play button find and click on the "Objectives" button.

Follow the instructions in the Objectives button. Text balloons will appear to guide you.

Making the proper procedural security choice completes phase one of this scenario.

1.2.3 Take a Quiz

The scenario now will ask a series of questions. To answer, you must press the "y" or the "n" key followed by the "enter" key as instructed in each question. If you get an answer wrong and the game ends, simply press the "r" key to restart it.

1.2.4 Fly Around the Office

You are done with this lab. Press the "k" key to bring up a keyboard shortcut list. That will tell you how to navigate around the office.

1.3 Clean Up

Exit the scenario by clicking the "Quit" button in the GAME screen.

The "View Log" button lets you view a log of what occurred during the game.

1.4 Play CyberCIEGE Outside the Lab

CyberCIEGE is also available to be played from workstations on the NPS domain. It is on a shared server and can be accessed as follows from any PC on the domain:

- login to the domain as yourself
- Map a drive to: \\kiska\Groups2$\CyberCIEGE
    - Right click on MyComputer
    - Select "Map Network Drive"
    - select the drive name (something like "u:" will not conflict with other mappings)

- In the "Folder" field, enter: \\kiska\Groups2$\CyberCIEGE

Finally, CyberCIEGE is available on CD for installation on home computers and laptops. See http://cisr.nps.edu/cyberciege/updates for system requirements and updates.

END OF LAB